UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,167	11/05/2003	Nancy Cam Winget	72255/00006	7272

23380 7590 06/16/2008
TUCKER ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2135	

NOTIFICATION DATE	DELIVERY MODE
06/16/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@tuckerellis.com
mary.erne@tuckerellis.com

Office Action Summary	**Application No.** 10/702,167	**Applicant(s)** WINGET ET AL.	
	Examiner SUMAN DEBNATH	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,26 and 28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16, 26 and 28* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-16, 26 and 28 are pending in this application.

2. Claims 1 and 9 are presently amended.

3. Claims 17-25 and 27 are cancelled.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-16, 26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Funk (Paul Funk; Simon Blake-Wilson; “draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)”; Internet-Draft PPPEXT Working Group; Nov. 2002, p. 1-40) (hereinafter “Funk”) and further in view of Palekar et al. (Pub. No.: US 2003/0226017 A1) (hereinafter “Palekar”).

6. As to claim 1, Funk discloses a method of secure communication comprising: establishing a secure tunnel between first and second parties using an encryption algorithm that establishes an encryption key (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2);

authenticating .the second party with an authentication server over the secured tunnel establishing an authentication key (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2 and Page 20, section 10);

verifying by the first party that the second party possess the same encryption and authentication keys as the first party (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10); and

provisioning a network access credential to the second party using the secured tunnel, responsive to the verifying the second party possess the same encryption and authentication keys as the first party ("The keying material is developed implicitly between client and TTLS server based on the results of the TLS handshake; the TTLS server will communicate the keying material to the access point over the carrier protocol" –e.g. page 12-13, sections 6-6.2, see also Pages 9-10, section 4.3; Pages 11-16, section 6-7, Page 20, section 10).

Although Funk teaches authenticating the second party (page 12-13, sections 6-6.2, see also Pages 9-10, section 4.3; Pages 11-16, section 6-7, Page 20, section 10), Funk is silent on authenticating a second time by the second party, wherein the second authentication is performed using the provisioned network access credential; wherein access to the second party to the network is denied unit the second party successfully authenticates using the provisioned network access credential. However, Palekar discloses authenticating a second time by the second party, wherein the second authentication is performed using the provisioned network access credential ([0007], [0062], "allowance of both communicating endpoints to verify that the other had calculated the same parameters"); wherein access to the second party to the network is denied unit the second party successfully authenticates using the provisioned network access credential ([0007], [0062], "allowance of both communicating endpoints to verify that the other had calculated the same parameters").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention made to modify the teaching Funk as taught by Paleker in order to increase the security of data communication over public network and maintain the integrity of both parties that communicate.

7. As to claim 9, it is rejected using the same rationale as for the rejection of claim 1.

8. As to claims 2 and 10, Funk discloses wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation (Pages 4-5, section 2).

9. As to claims 3 and 11, Funk discloses wherein the encryption algorithm is an asymmetric encryption algorithm (Page 9-10; sections 4.2-4.3; Page 28, section 12).

10. As to claims 4 and 12, Funk discloses wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel (Page 9-10; sections 4.2-4.3; Page 28, section 12).

11. As to claims 5 and 13, Funk discloses wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange (Pages 36-37, section 14).

12. As to claims 6 and 14, Funk discloses wherein the step of authenticating is performed using Microsoft MS-CHAP v2 (Pages 11-12; section 6; Pages 23-24, section 10.2.4).

13. As to claims 7 and 15, Funk discloses further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties (Pages 11-16, sections 6-7).

14. As to claims 8 and 16, Funk discloses wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI) (Pages 9-10, sections 4.2-4.3, Page 20, section 10).

15. As to claim 26, Funk discloses wherein the verifying further comprises hashing the first party encryption key and the authentication key to produce a first hash ("...the master secret and random values" –e.g. Page 20-21 and Page 23); hashing the second party encryption key and the second party authentication key to produce a second hash; verifying the first and second hash are the same (Page 20-21 and Page 23, "the TTLS server must verify that the value of the MS-CHAP-Challenge AVP and the value of the Ident in the client's MS-CHAP-Response AVP are equal to the values generated as challenge material" –e.g. Page 23. Funk teaches the concept of hashing by using MS-CHAP-V2).

16. As to claim 28, Funk discloses further comprising invalidating a secure credential for the second party responsive to a failure of one of the group consisting of establishing the secure tunnel, authentication, and verifying second party has the same encryption and authentication keys ("If either item does not match exactly, the TTLS server must reject the client" –e.g. Page 23).

Response to Amendment

17. Applicant has amended claims 1 and 9, which necessitated new ground of rejections. See rejections above.

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135